基于 T_NAG 模型的攻击路径预测方法研究 *

翟海霞，卢月萌†，王　辉，敖　山
(河南理工大学 计算机科学与技术学院，河南 焦作 454003)

摘　要：为了更好刻画攻击者的攻击轨迹，设计出一种基于 T_NAG(time attribute network attack graph)模型的路径预测方法。首先，提出新的攻击图模型 T_NAG，根据实时行为轨迹对攻击者能力加以区分；其次，依据攻击者具有不同能力的特性，提出攻击意向的概念，统筹考虑操作风险与攻击收益，将时间衰减参数引入到攻击意向计算中，并设计出一种基于攻击者能力的漏洞利用率量化方法；最后，将攻击意向与漏洞利用率进一步融入到对路径可达概率的考量中，给出预测攻击路径的 IntenAbi-PathPre 算法。实验结果表明，该方法可以有效去除攻击图中的冗余，并且使攻击路径预测的准确性得到明显提高。

关键词：攻击图；路径预测；攻击者意向；路径可达性
中图分类号：TP　　doi: 10.19734/j.issn.1001-3695.2019.11.0701

Research on attack path prediction method based on t_nag model

Zhai Haixia, Lu Yuemeng†, Wang Hui, Ao Shan
(*College of Computer Science & Technology*, *Henan Polytechnic University*, *Jiaozuo* 454003, *Henan*, *China*)

Abstract: In order to depict the attacker's attack trajectory better, this paper proposed a path prediction method based on T_NAG(time attribute network attack graph) model. First of all, proposed a new attack graph model T_NAG to distinguish the attacker's ability according to the real-time behavior trace. Secondly, according to the characteristics of the attacker's different capabilities, proposed the concept of attack intention, considered the operation risk and attack profit as a whole and introduced the time decay parameter into the intention calculation, and designed a vulnerability utilization quantification method based on the attacker's capabilities. Finally, further integrated attack intention and vulnerability utilization into the consideration of path reachability probability, and given the IntenAbi-PathPre algorithm to predict the attack path. The experimental results show that this method can effectively remove the redundancy in the attack graph and improve the accuracy of attack path prediction.

Key words: attack graph; path prediction; attacker's will; path accessibility

0　引言

互联网的广泛应用使社会生产和人类生活更加高效便利，但是存在于复杂网络中的大量漏洞必然会引发出诸多网络安全威胁。国家互联网应急中心(CNCERT)发布的《2018 年我国互联网网络安全态势综述》中指出，2018 年计算机病毒、蠕虫、木马程序等恶意程序日均传播超过 500 万次[1]。2014 年以来 CNVD 漏洞平台收录的安全漏洞数量逐年上升，平均增长率高达 15%。美国 Positive Technologies 公司公布的最新网络安全报告显示，2018 年全球范围内有 7.65 亿用户遭受到不同程度的网络攻击。根据以色列 Radware 公司发布的最新调查报告，34%的用户在接受采访时认为应用程序漏洞是 2019 年严重影响网络安全性的首要因素[2]。

对于企业级网络来说，在配置防护措施时需要预知网络中存在的风险，从而有针对性地保护重点区域和节点。而攻击图技术[3]可以直观地展示攻击方可能采取的攻击路径，通过构建攻击图模型对网络的安全性进行分析，网络管理者不仅可以筛选出需要加强保护的重要节点[4,5]，还可以在攻击发生时预测后续的攻击目标[6,7]。

近年来，众多学者不仅以攻击图模型作为分析网络安全性的工具，也基于不同角度提出了很多评估网络安全性和预测攻击意图的方法。叶子维等人[8]对攻击图模型的基本要素进行分析，给出了攻击图的定义和简要介绍，并总结了攻击图模型在应用方面的现状和存在的问题。秦虎等人[9]以攻击模式库和网络环境的配置为依据，在对攻击行为进行分析后，认为攻击者攻击能力的变化应该以取得权限的提升为标志，并提出基于攻击者能力提升模型的攻击图生成方法。Mohammad 等人[10]指出单纯使用静态漏洞概率来预测风险的局限性，在预测过程中使用对实时入侵警报和依赖关系图等信息要素进行提取分析，并提出了一种基于信息整合的网络攻击预测方法。通过以上的研究成果，本文可以得知：一方面攻击者在对漏洞的利用程度、规避攻击可能造成的风险等方面的水平高低存在的差异对网络的安全性是有一定影响的，并且影响程度可以通过攻击过程中客观因素的变化情况得知。另一方面，攻击行为产生的大量信息要素都可以辅助于对攻击行为的预测，但前提是需要将各项要素对于路径可达性和网络安全性的影响关系和变化趋势进行分析，并使用恰当的数学模型表示。

文献[11]基于攻击图模型提出了一种攻击路径生成算法。假设期望得到 K 个可达概率最大的路径，根据 K 值动态调整概率分布，通过计算攻击路径的累积可达概率实现对路径的预测。该算法在量化节点可达概率时，只考虑漏洞利用率

收稿日期：2019-11-24；**修回日期：**2020-01-10　**基金项目：**国家自然科学基金资助项目(61300216)；全国教育科学规划教育部重点课题资助项目(DFA170292)；河南省软科学研究计划资助项目(182400410147)

作者简介：翟海霞(1976-)，女，河南济源人，副教授，硕导，博士，主要研究方向为主要研究方向为网络安全；卢月萌(1995-)，女(通信作者)，河南南阳人，硕士研究生，主要研究方向为主要研究方向为网络安全(347351225@qq.com)；王辉(1975-)，男，河南焦作人，副教授，硕导，博士，主要研究方向为主要研究方向为计算机网络及网络安全等；敖山(1971-)，男，四川丰都人，副教授，硕导，博士，主要研究方向为主要研究方向为网络安全.

一个因素，缺乏对攻击事件本身的建模与分析。

文献[12]使用贝叶斯攻击图对网络动态风险进行评估，充分考虑到了攻击事件对于节点后验概率的动态影响，并运用贝叶斯推理的方法预测攻击路径。但是攻击事件的成功概率依靠专家经验，忽略了攻击事件发生后资源节点被占有的概率与攻击行为的具体情景相关，影响预测的准确性。

文献[13]将攻击图映射为 Markov 链，并提出 Markov 链中节点的状态转移概率算法。但状态转移概率的计算依赖于 CVSS 中的漏洞可用性指标这一静态因素，而没有考虑到攻击者能力对漏洞可用性的动态影响，所以攻击路径的预测准确度较低。

文献[14]假设攻击者是理性的，在定性分析影响攻击代价和收益的因素的基础上，分别给出了攻击代价和攻击收益的量化算法，并将代价-收益模型引入到节点可达性的计算中，从而实现对攻击路径的预测。但是在量化节点可达性的时候没有考虑到攻击耗时产生的影响。

文献[15]提出了一种基于风险流攻击图的网络风险评估方法，风险流攻击图不仅用来描述网络结构，同时也可以对攻击场景建模。论文着眼于分析入侵事件与网络风险之间的联系，然后提出基于模糊评价的风险评估方案。但是从入侵事件中提取到的大量信息只用来量化网络风险，没有利用相关信息对攻击行为的收益和耗时、攻击者表现出的水平差异等其他影响网络安全性的因素加以分析。

文献[16]设计一种基于时间增益补偿率的攻击路径优化方案，将攻击行为所反映的时间特征融入到攻击图模型当中，认为攻击耗时可以被看做攻击成本中的时间成本因素，重点分析攻击耗时与节点可达概率的关联性，根据对时间成本的增长情况的量化消除路径冗余。但是文中时间成本的量化值主要取决于元操作序列耗费时长的累加，这导致了时间成本的值域不可控制，对风险分析的准确性造成影响。

针对已有研究成果对影响网络安全性的因素考虑不全面，预测准确度低等情况，本文提出了基于攻击者意向的攻击图模型 T_NAG，对影响攻击者攻击意向的因素逐一进行分析并给出量化方法，依据攻击者能力等级对漏洞利用率计算方法加以改进，最后将攻击者意愿与漏洞利用率结合对攻击图进行优化，并计算路径的可达概率，通过比较路径可达概率值预测攻击者可能采取的攻击路径。

1 攻击图 T_NAG 模型

为了分析攻击者行为，以便于更加准确清楚地描述攻击图模型，首先引入一些变量的定义。

定义 1 网络安全漏洞 v 使用二元组(vID , $vInfo$)表示。其中 vID 是漏洞的唯一编号； $vInfo$ 表示对该漏洞的描述。

定义 2 网络设备 h 包括网络中的主机和防火墙等，用四元组(hID ， $Services$ ， V ， $hValue$)表示。其中 hID 表示网络设备的编号； $Services$ 表示网络设备上运行服务的集合； V 表示该网络设备的脆弱性信息集合，对于任一 $v \in V$ 由定义 1 描述； $hValue$ 表示网络设备的资产价值。将网络中所有设备组成的集合用 H 表示。

定义 3 攻击意向 κ 表示对攻击者发起攻击的主观倾向的量化，记作 $\kappa \in (0,1)$ ，数值越大表示攻击意向越强。

定义 4 漏洞可利用性 vul 表示攻击者利用特定漏洞发起原子攻击的难易程度，记作 $vul(v) \in (0,1)$ ， vul 值越大，漏洞 v 可利用性越强，发起原子攻击的难度越低。

根据已有研究成果，攻击图模型主要分为状态攻击图和属性攻击图。其中属性攻击图[17]以影响网络安全性的要素作为独立顶点，有效地控制了生成攻击图的规模，相比于状态攻击图，更适用于大型网络。为了体现时间参数对于攻击意向的影响，和攻击意向对于路径预测的影响，本文以属性攻击图为基础提出了引入时间属性和攻击意向的网络攻击图 T_NAG 模型，用来评估网络安全性。

定义 5 攻击图 $T_NAG(R, A, E, \vartheta, \varsigma, W)$ ，其中：

a) R 为资源节点集合，记为 $R = \{R_0 \cup R_{mid} \cup R_g\}$ 。其中 R_0 为起始资源节点集合，即初始时刻攻击者占有资源节点的集合； R_{mid} 为中间资源节点集合，也就是攻击者从初始资源节点开始到占有目标资源节点的过程中需要占有的中间资源节点的集合； R_g 为目标资源节点集合，即攻击者最终期望占有的资源节点集合。$r \in R$ 表示独立的资源节点，记为 r = (rID ， hID ， jur)，其中 rID 表示资源节点的唯一编号， hID 表示资源所属网络设备的编号， jur 表示资源的具体内容如某一级别的权限，或者信任关系等。

b) A 为攻击节点集合，记为 $A = \{a_1, a_2, ..., a_n\}$ 。其中 $a_i \in A$ 表示攻击者发动的原子攻击，记作 a_i = (aID ， vID ， $aSTime$ ， $aETime$)。其中 aID 表示攻击名称， vID 表示攻击所利用漏洞的编号， $aSTime$ 表示攻击开始的时刻， $aETime$ 表示攻击结束的时刻。

c) E 表示攻击图中的有向边集合，记为 $E = \{E_1 \cup E_2\}$ 。其中 $E_1 = \{e_{ij} \mid e_{ij} = <r_i, a_j>, r_i \in R_0 \cup R_{mid}\}$ ，表示攻击者在占有前序资源节点 r_i 的条件下才能发动攻击 a_j ； $E_2 = \{e_{ji} \mid e_{ji} = <a_j, r_i>, r_i \in R_{mid} \cup R_g\}$ ，表示攻击者发动攻击 a_j 是为了占有后继资源节点 r_i 。

d) ϑ 为攻击标志集合。当 $\vartheta_{ij} \in \vartheta$ 且 $r_i, r_j \in R$ 时，如果 $\vartheta_{ij} = true$ ，攻击者可能在获得资源 r_i 之后对资源节点 r_j 发动攻击，如果 $\vartheta_{ij} = false$ ，表示攻击者放弃对资源节点 r_j 发动攻击。

e) ς 表示节点与前驱节点之间的逻辑关系， $\varsigma \in \{and, or\}$ 。如果 $\varsigma(a_i) = and$ ，那么攻击 a_i 发生的前提是攻击者占据所有前驱节点资源；如果 $\varsigma(a_i) = or$ ，表示攻击者占据任意前驱节点资源，攻击 a_i 就可能发生。如果 $\varsigma(r_i) = and$ ，那么资源节点 r_i 被占有的前提条件是所有前驱节点攻击发生；如果 $\varsigma(r_i) = or$ ，只要前驱节点任意攻击发生，资源节点 r_i 就可能被占有。

f)攻击权重集合 W 。对于 $e \in E_2$ ，都有对应的权重 $w \in W$ ，记为 $w(e) = (vul, \kappa)$ ，其中 vul 表示漏洞可利用性， κ 表示攻击者意向。

定义 6 攻击者能力等级 Att_abi 表示对不同攻击者攻击能力的统一量化，记作 $Att_abi \in \{low, mid, high\}$ 。

定义 7 攻击路径 $PATH$ 由二元组组成，记作 $PATH = (Seq, Att_abi)$ 。其中 Seq 表示路径序列， Att_abi 表示攻击者能力等级。对于任一目标节点 $r_i \in R_g$ ，如果从起始节点 r_0 开始，存在一组有序节点序列 $r_0, a_1, r_1, a_2, ..., a_m, r_n$ ，序列中任意两个相邻节点的边满足 $<r_i, a_j> \in E_1$ 或者 $<a_j, r_i> \in E_2$ ，那么就将节点序列称作一条路径序列，记做 $Seq = \{<r_0, a_1>, <a_1, r_1>, ..., <a_1, r_n>\}$ 。

定义 8 攻击模式 表示攻击者实施攻击的行为的一般方式。攻击行为发生的前提是依赖特定资源比如访问被攻击主机上某项服务，获得被攻击主机的信任等。攻击的目的是进一步获取更多资源。如图 1 所示，在连续攻击中上一次攻击获取的资源就是下一次攻击发生的前提资源。攻击者的一系列攻击行为，通过资源节点有机地联系在一起，形成了特定的攻击意图。

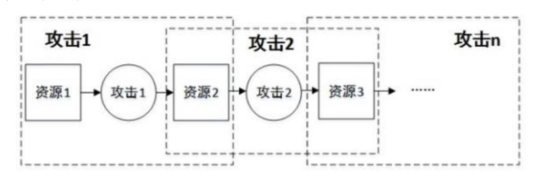


图 1 攻击过程示意

Fig. 1 Attack process schematic

定义 9 攻击子路径 根据对攻击模式的分析，由于原子攻击 a 的完成总是依赖于前提资源 r_i ，而攻击的目的是后继

资源 r_j，所以将 $<r_i,a>\in E_1$ 和 $<a,r_j>\in E_2$ 整体考虑，作为路径的最小单元，使用 $r_i\rightarrow a\rightarrow r_j$ 表示。

2　攻击路径预测

2.1　攻击者能力等级

考虑到实际应用中不同能力的攻击者对于同一漏洞的利用程度存在差别，从而对攻击结果产生一定的影响，所以攻击成功的概率不仅与复杂度有关，也与攻击者能力相关。本文以攻击所需漏洞的脆弱性利用难度为根据，对攻击者能力作出区分。这样可以避免以主观经验确定攻击者能力的传统做法，提高结果的可信程度。

文献[18]提出并证明了由同一攻击行为结果推断出的攻击者能力等级的概率分布正比于攻击者实施攻击成功或失败的概率分布。CVSS[19]中使用攻击复杂度参数 Ac 将脆弱性被利用的难度分为 Low， Mid， $High$ 共 3 个等级，攻击成功的概率越高，攻击复杂度 Ac 的取值就越高。因此定义攻击者的能力等级等于攻击者实施攻击过程中利用漏洞集合中难度最高的漏洞的等级。假设攻击者发动的一系列连续攻击所利用的漏洞集合为 V，攻击者能力等级的计算公式如下：

$$Att_abi=\max(Ac(v)),v\in V \tag{1}$$

2.2　攻击者意向

通常，攻击者对攻击路径的选择不仅受到操作风险和攻击收益的影响，同时也受到动态因素如攻击者能力和攻击耗时的影响。实施不同攻击行为的攻击者可能具有不同的攻击能力，而能力等级会对攻击者意向的取值产生影响。假设攻击者是理性的，那么在攻击过程中必然会考虑时间成本因素，如果攻击行为已经消耗很长的时间，但是却没有进展，那么攻击者的攻击意向就会大幅降低。根据上述分析，引入能力因子和时间因子，对攻击者意向进行动态的分析与评估。

2.2.1 风险因子

风险因子 $Risk$ 表示单个攻击行为造成风险的严重程度。风险因子的取值与攻击所利用漏洞自身的属性相关，一个漏洞的影响性越大，利用该漏洞发起的攻击行为的风险就越高。攻击造成的风险越严重，攻击行为被网络管理者发现的可能性就越大，因此攻击成功需要花费的代价就越高，攻击者意向就会相应减弱。因此可以使用漏洞影响性来衡量攻击产生的风险。设攻击 a 利用的漏洞为 v，参照 CVSS 中漏洞影响性的计算公式，得到风险因子的计算公式：

$$\begin{aligned}Risk(a)&=Impact(v)\\&=10\times(1-C)\times(1-I)\times(1-A)\end{aligned} \tag{2}$$

其中 $Impact$、Atr、$Atr=\tau^{Time}\times\theta(a)$ 分别表示 CVSS 中漏洞的机密性指标取值、完整性指标取值和可用性指标取值。攻击风险 $Impact$ 的取值在 0-10 之间，取值越高表示漏洞造成的影响越大。

2.2.2 能力因子

能力因子 Atr 表示攻击者能力对风险因子的影响程度。

$$Atr=\tau^{Time}\times\theta(a) \tag{3}$$

式(3)是前人提出的能力因子的计算方法，其中 τ 是能力系数，$Time$ 为攻击次数，$\theta(a)>1$ 是风险系数，其值由专家经验给出。这种方法使用攻击次数量化攻击能力，没有考虑不同攻击者之间的能力差距。如果攻击者能力等级较高，就会使攻击复杂程度有所减少，由于攻击者能力等级与攻击风险成反比关系，所以攻击者发动攻击的意向加强。改进后的能力因子计算公式如下：

$$Atr=\frac{\exp\sqrt{\tau^{Att_abi}}-\varepsilon}{e} \tag{4}$$

其中 $\tau<1$ 是能力系数，Att_abi 表示攻击者能力等级，调节因子 $\varepsilon\in(0,1)$ 用来对能力因子的取值进行修正，因此 $Atr\in(0,1)$。与传统方法不同，如果攻击者能力较弱，根据式(1)，能力等级 Att_abi 较低，τ^{Att_abi} 取值接近于 0，能力因子 Atr 的值不会过低，而是接近于 1。此外能力因子取值范围更加平缓，避免出现能力等级不同的情况下能力因子取值差距过大的情况。

2.2.3 攻击收益

使用攻击收益衡量原子攻击成功的情况下，攻击者获得的资源对其攻击意图的有利程度。攻击收益有以下性质：

a) 攻击获得收益的价值最多只能等于攻击目标资产 r_j 的价值。

b) 收益价值量是根据攻击行为对目标主机造成的影响，即获取目标主机权限的变化情况，结合目标资源价值共同确定。

攻击行为造成安全事件的发生。根据事件发生的形式和影响范围，安全事件一般可分为信息泄露、远程登录、绕过身份认证、获得用户权限和获得 Root 权限共 5 种类型。由于形式和影响范围的差异，不同类别安全事件的严重程度存在差别，而安全事件的严重程度与攻击者获得的收益是正相关的。事件越严重，意味着通过攻击获取了更高的操作权限，从而得到更高比例的收益。

所以根据安全事件的严重程度，将攻击收益分为 G1~G5 共 5 个等级，其中 G1 表示最低等级的收益，G5 表示最高等级的收益。为了便于计算，需要将收益等级量化，故定义收益因子 $\rho\in(0,1]$，表示通过攻击行为，攻击者获得收益与目标资源价值的比值，收益等级越高，收益因子的取值就越大。收益等级、安全事件名称和收益因子取值的对应情况由表 1 给出。目标资源的价值根据目标资源的重要性确定，资源越重要，其价值越高。那么通过攻击 Atr 得到的收益 $Gain$ 为

$$Gain(a)=(\rho_{now}-\rho_{pre})\times\omega(r_j) \tag{5}$$

其中 $\rho_{now}(a)$ 是如果攻击成功，攻击者将要达到的收益等级所对应的收益因子，$\rho_{pre}(a_k)$ 是本次攻击发生之前，攻击者已经获得的收益等级所对应的收益因子，$\omega(r_j)$ 是攻击的目标资源 r_j 的价值。

表 1　收益等级表

Tab. 1　Income scale

收益等级	属性	收益因子
G1	信息泄露	0.2
G2	远程登录	0.3
G3	绕过身份认证	0.4
G4	获得用户权限	0.7
G5	获得 Root 权限	1.0

2.2.4 时间系数

除了风险、能力和收益这三个因素外，攻击所耗费时长也会对攻击意向产生一定程度的影响。

本文定义时间系数 $f_t(e)$，以表示攻击时长对攻击意向的影响。具体来说，攻击所花费的时长是影响攻击意向的主要因素。漏洞利用难度一定的条件下，攻击时间则越短，攻击意向则越强。随着花费时间的增多，攻击者意向逐步降低。当花费时间非常长的情况下，时间系数取值接近于 0。此外定义时间衰减系数 α，用来调节时间系数的值，使时间系数的取值更加符合一般情况。使用时间系数 $f_t(e)$ 量化时间衰减，计算公式如下：

$$f_t(a)=\frac{1}{1+\alpha\ln|aNTime-aSTime|} \tag{6}$$

其中 $Risk$ 是时间衰减系数，取值根据攻击耗时的具体情况确定。如果攻击者在发动的攻击耗时较长，那么 α 适合取较小的值；耗时较短，那么 α 适合取较大的值。$aNTime$ 表示当前时刻，$aSTime$ 表示攻击开始时刻。$f_t(a)$ 的取值范围是 $[0,1]$。相比于前人提出的计算方法，时间系数 $f_t(a)$ 有明确的取值范围和优化的计算方法，从而更好地反映时间成本对于攻击意向

的影响。

2.2.5 攻击者意向分析

使用传统方法分析攻击的可能性时，往往只量化攻击付出的代价，如果攻击代价高于设定的阈值，就放弃对该节点的攻击。虽然某些攻击风险较大，所需代价偏高，但是通过攻击可能会得到更高价值的资源，这种情况下攻击者的意向仍然较强。以漏洞风险值与攻击收益的比值为基础，结合攻击者能力和时间系数对攻击意向影响性的分析，提出新的攻击者意向计算公式：

$$\kappa(a)=f_t(a)\frac{Gain(a)-Risk(a)\times Atr}{Gain(a)} \tag{7}$$

其中 $Gain$ 为收益，$Risk$ 为漏洞风险值，Atr 为能力因子，κ 表示攻击者意愿，取值越大表示攻击者意愿越强。规定只有当 κ 达到一定的值，攻击者才有可能发动攻击。攻击过程中，时间成本动态变化，随着时间成本增多，$f_t(a)$ 值逐渐变小，攻击意向逐渐降低，直到攻击意向 κ 的取值小于阈值，即表示放弃攻击。

2.3　路径预测算法

2.3.1 路径可达概率

在获得攻击路径相关信息并确定攻击者意向计算方法的基础上，给出路径可达概率计算的方法，结合条件概率与攻击者意向综合考虑子路径可达性，进而得出整条路径可以达到的攻击阶段和可达概率。由于 CVSS 中攻击复杂度 Ac 表示漏洞的利用率，根据 2.1 节的分析，结合 CVSS 中攻击复杂度 Ac 各属性的取值，可以得出不同能力等级的攻击者对漏洞的利用率 $P(Ac,Att_abi)$ 的取值，如表 2 所示。

表 2　基于能力等级的漏洞利用率量化值

Tab. 2　Quantitative value of vulnerability utilization based on capacity level

Ac	$P(Ac,Att_abi)$		
	$Att_abi=low$	$medium$	$high$
低	0.56	0.63	0.71
中	0.49	0.56	0.63
高	0.41	0.49	0.56

依据表 2 给出的漏洞利用率的取值方法，给出计算漏洞可用性的公式：

$$Vul(v)=2\times Av\times P(Ac,Att_abi)\times Au \tag{8}$$

其中 Av 表示 CVSS 中漏洞 v 的攻击途径，Au 表示 CVSS 中漏洞的认证指标，即利用漏洞发起攻击所需的认证次数。$P(Ac,Att_abi)$ 表示在已知漏洞复杂度 Ac 取值和攻击者攻击能力 Att_abi 的前提下得出的漏洞利用率的取值。对于一个漏洞来说，Vul 值越小，利用该漏洞发起的攻击行为的难度越大。

使用可达概率量化攻击成功时单个状态节点受到威胁的可能性。原子攻击相关的子路径使用 $r_i\to a\to r_j$ 表示，设攻击 a 利用漏洞 v 发起攻击，r_j 是期望通过攻击占有的资源节点，r_i 是发起攻击所需前提资源集合，结合攻击者意向，对于原子攻击 a，子路径 $r_i\to a\to r_j$ 的可达概率：

$$P_{kd}(r_i\to a\to r_j)=Vul(v)\times\kappa(a) \tag{9}$$

定义 10　路径可达概率　假设路径 $PATH$ 的路径序列 $Seq=\{<r_1,a_1>,<a_1,r_2>,\ldots,<a_m,r_n>\}$ 可以拆分为数条子路径，每条子路径对应一次原子攻击过程，设子路径表示为 $r_i\to a\to r_j$，路径可达概率公式如下：

$$\begin{aligned}P(PATH)&=\prod_{i=1}^{m}[P_{kd}(R_i\to a\to r_j)]\\&=\prod_{i=1}^{m}[Vul(v_k)\times\kappa(a_i)]\end{aligned} \tag{10}$$

2.3.2 路径预测算法

基于 2.3.1 节中路径可达概率的计算方法，本文设计了路径预测算法(IntenAbi-PathPre)，通过计算子路径可达概率消除冗余的攻击路径，然后筛选出可达概率最高的路径即为攻击者优先考虑的路径。

算法 1　路径预测算法

输入：攻击图中攻击路径集合 Path，攻击边 $\langle a_i,r_j\rangle$ 的漏洞利用率 $\mathrm{Vul}(v)$，攻击意向 $\kappa(a)$。

输出：预测路径 U_Path。

1 for each $\mathrm{Path}_i\in\mathrm{Path}$
2 $P_{kd}(\mathrm{Path}_i)=1$
3 　for each $e\in\mathrm{Path}_i$ //遍历路径中的边
4 　　if($e\in E_2$)//如果当前边是攻击边
5 　　　$R_i=\mathrm{pre}(\mathrm{Dot}_1)$，$a=\mathrm{Dot}_1$，$r_j=\mathrm{Dot}_2$
6 　　　$P_{kd}(R_i\to a\to r_j)=\mathrm{Vul}(v)\times\kappa(e)$
7 　　　if($P_{kd}(R_i\to a\to r_j)<\psi$)
8 　　　　$\xi_{ij}=\mathrm{false}$
9 　　　　delete Path_i
10 　　　　break
11 　　　else $\xi_{ij}=\mathrm{true}$
12 　　　end if
13 　　　$P_{kd}(\mathrm{Path}_i)=P_{kd}(\mathrm{Path}_i)\times P_{kd}(R_i\to a\to r_j)$
14 　　end if
15 　end for
16 end for
17 order Path_i in Path by P_{kd}
18 U_Path←Path
19 return U_Path

算法第 3~14 行对路径中的各边进行遍历。其中 4~6 行表示如果当前边代表攻击，那么计算漏洞利用率和动态的攻击意向，结合两者得出子路径可达概率。第 7-10 行表示如果子路径可达概率小于阈值，那么攻击者放弃攻击该路径，将相应路径从路径集中删除。第 11~13 行表示如果可达概率大于阈值，那么将子路径可达概率累乘得出子路径所属路径可达概率。17~19 行表示在所有路径的可达概率计算完成后，根据路径可达概率值的大小对路径的优先级排序，优先级越高说明路径越有可能被攻击者选择，其结果供网络管理员参考。

3　实验验证与分析

3.1　实验网络环境

如图 2 所示，实验网络分为两个区域：DMZ 区和 Inside 区，使用防火墙将不同区域隔离。DMZ 区有 1 台网络服务器 H1。Inside 区有 4 台服务器，分别是 Ftp 服务器 H2，主机 H3，主机 H4，数据库服务器 H5。在小型局域网中，入侵者使用主机 H0 远程访问目标网络。DMZ 区的 H1 可以与外部网络相连，也可以访问 Inside 网络中的 FTP 服务器 H2、主机 H3 和主机 H4。Inside 区不能被外部网络直接访问，Inside 内部 FTP 服务器 H2、主机 H3 可以访问 H4，主机 H4 可以访问数据库服务器 H5。

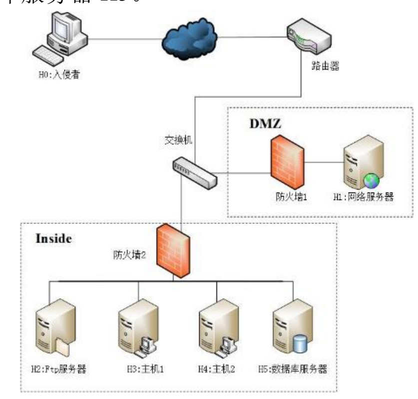


图 2　网络结构图

Fig. 2　Network structure

表 3　漏洞信息与攻击编号对照表

Tab. 3　Vulnerability information and attack number contrast

服务器	服务	编号	攻击编号	Ac
H1	Telnet	CVE-2016-7115	a1	low
H2	FTP	CVE-2018-19999	a2	low
		VE-2013-1324	a3	mid
H3	Windows	CVE-2011-0638	a4	high
	SSH	CVE-2018-1000805	a5	low
H4	FTP	CVE-2018-19999	a6,a7,a8	mid
	HTTP	CVE-2019-7228	a9	low
H5	SQL	CVE-2019-1010201	a10	low

各主机运行服务名称及对应漏洞如表 3 所示。Ac 为 CVSS 中相应漏洞的复杂度，攻击编号表示利用相应漏洞发起的攻击编号。

3.2　实验过程

给出网络配置信息，利用攻击图生成工具 MulVal 绘制的攻击图如图 3 所示。根据绘制好的网络攻击图，生成攻击目标为主机 H5 的所有路径，一共有 7 条路径可以到达主机 H5。路径信息如表 4 所示。

由于 PATH$_1$ 中攻击 a3 复杂度为中等，其余 3 次攻击 a1,a7,a10 复杂度都是低等，根据式(1)，沿着该路径发起攻击所需能力为中等，如果攻击者选择该条路径，那么攻击者能力就为中等。同理，如果攻击者选择 PATH$_3$ 或 PATH$_4$，整个路径中复杂度最高的攻击是 a4，且其复杂度为高等，那么攻击者能力为高等。如果攻击者选择了除 PATH$_1$、PATH$_3$ 和 PATH$_4$ 以外的其他路径，那么攻击者能力为低等。

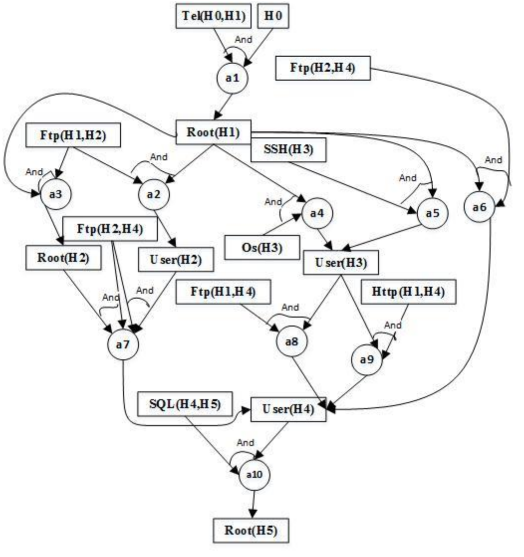


图 3　网络攻击图

Fig. 3　Network attack graph

表 4　路径信息表

Tab. 4　Path information table

名称	路径
PATH$_1$	(H1,a1)→(H2,a3)→(H4,a7)→(H5,a10)
PATH$_2$	(H1,a1)→(H2,a2)→(H4,a7)→(H5,a10)
PATH$_3$	(H1,a1)→(H3,a4)→(H4,a8)→(H5,a10)
PATH$_4$	(H1,a1)→(H3,a4)→(H4,a9)→(H5,a10)
PATH$_5$	(H1,a1)→(H3,a5)→(H4,a8)→(H5,a10)
PATH$_6$	(H1,a1)→(H3,a5)→(H4,a9)→(H5,a10)
PATH$_7$	(H1,a1)→(H4,a6)→(H5,a10)

以主机的重要程度为依据，将 H1、H3 和 H4 的资产价值定为 40，H2 的资产价值为 30，H5 的资产价值为 60。根据专家经验取能力系数为 0.5。式(4)中的调节因子和式(7)中的时间衰减因子通过预先的样本训练得出。通过入侵检测系统的警报信息，得到攻击耗时，然后与公式中其他参数一起代入到攻击意向分析公式中计算。

3.3　实验结果分析

首先分析时间衰减系数对攻击意向的动态影响。根据式(6)，时间因子 f_t 的变化情况如图 4 所示，在时间消耗合理(0-60 min)的情况下，时间因子取值的变化比较小，总体趋近于 1，对攻击者意向的制约较小，所以在其他参数不变的情况下攻击者意向相对强烈。当攻击消耗的时间超过合理区间时并逐渐增多时，有了非常明显的下降趋势，直到消耗时间达到 120 分钟左右的时候已经下降到一个非常低的值，并且随着时间继续增加，攻击意向仍在缓慢下降。

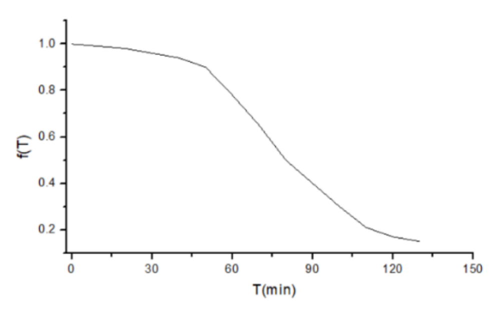


图 4　时间因子取值变化

Fig. 4　Change of time factor

经过反复实验，将攻击意向的阈值设为 0.2。由于路径 PATH3 中的子攻击 a8 耗时大约 110min，导致时间衰减系数降到 0.17，从而攻击意向降为 0.16，小于阈值，所以攻击者放弃该条路径。路径 PATH5 上的子攻击 a8 耗时也比较长，大约 100min，时间衰减系数降到了 0.2，攻击者的攻击意向降为 0.14，所以 PATH5 也被攻击者放弃。通过引入时间衰减系数，有效实现了对已有路径的优化。

其次，攻击意向不仅受到攻击耗时的影响，同时也受到攻击者能力的影响。选择 PATH5 的攻击者能力为低级，而选择 PATH3 的攻击者能力为高级。根据式(4)，能力等级越低，能力系数取值越高，能力因子取值越大。根据式(7)，能力因子越大，对攻击造成风险的影响越小，操作带来的风险就越高。因此选择 PATH5 的攻击者发动攻击 a8 时付出的代价比较高，在 PATH5 中 a8 时间衰减系数略高于 PATH3 中 a8 的前提下，攻击者对 PATH5 的意向反而比 PATH3 还要略低。

表 5　PATH1 计算信息表

Tab. 5　PATH1 computational information

原子攻击	(H1,a1)	(H2,a3)	(H4,a7)	(H5,a10)
成功概率	0.89	0.79	0.71	0.89
攻击意向	0.89	0.85	0.89	0.92
累积概率	0.789	0.529	0.332	0.271

表 6　PATH6 计算信息表

Tab. 6　PATH6 computational information

原子攻击	(H1,a1)	(H3,a5)	(H4,a9)	(H5,a10)
成功概率	0.79	0.79	0.63	0.79
攻击意向	0.81	0.73	0.73	0.87
累积概率	0.639	0.368	0.168	0.115

以 PATH1 和 PATH6 为例说明单条路径可达概率的计算过程。这两条路径的第一步攻击和最后一步攻击是相同的，但是由于选择 PATH1 的攻击者能力为中等，PATH 6 的攻击者能力为低等，PATH1 中这两次单步攻击的成功概率和攻击意向都要略高于 PATH3。在单步攻击耗时均合理的情况下虽然攻击者能力一致，攻击所得的收益与承担风险的比值不相同，所以攻击者对同一条路径中的各个单步攻击的意向也不相等。对于单步攻击而言，收益比例相对较高的攻击者意向就会相对强烈。

设 P1 是未引入攻击者能力、攻击耗时和攻击意向时计算的路径可达概率结果，P2 是根据提出的改进算法得出的路径可达概率。根据表 4 给出的攻击图中所有路径的信息，分别在 P1 和 P2 下计算各路径的可达概率，结果如图 5 所示。

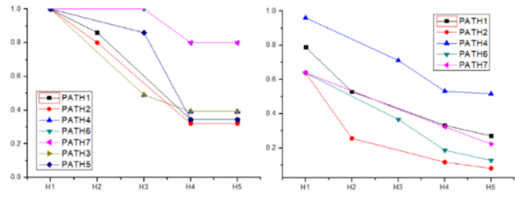


图 5 P1、P2 下各路径可达概率对比

Fig. 5 Comparison of reachability probability of each path under P1 and P2

从图 5 中可以看出，P1 下可达路径一共 7 条，但是 P2 下可达路径减少到 5 条，这是因为 2.3.2 节提出的 IntenAbi-PathPre 算法对路径的优化作用。根据前面的具体分析，由于 PATH3 和 PATH5 的攻击意向值低于阈值，优化后这两条路径被攻击者舍弃，减少了不同路径重合混淆的几率，使路径可达概率图更加清楚简洁。

此外，P1 下不同路径中各节点的可达概率取值相差比较小，在 H4 点及以后各路径已经混淆在一起，管理员识别危险路径的难度明显增加。但在 P2 中，在可达概率的计算方法中融入攻击者能力和攻击者意向之后，对于各路径来说，虽然路径可达概率的值不同程度地减小了，但是可达概率的变化趋势反而比较平缓，不同路径之间可达概率的差异更加分明。尽管在 H4 和 H5 位置可达概率的数值已经比较低，但是路径间差距非常明显，显然可以看出 PATH2、PATH4 两条路径的攻击概率更大，并且虽然选择这两条路径攻击的攻击者能力都比较强，路径之间可达概率差异仍然明显。此外，虽然利用路径 PATH7 进攻的攻击者能力为低，但是其入侵节点 H5 的成功概率仅次于 PATH2 和 PATH4，也是网络管理员需要防范的对象。

3.4 实验结果比较

为了进一步验证本文提出的基于 T_NAG 模型的攻击路径预测方法的有效性，查阅了大量研究网络攻击预测技术的相关文献。通过对比得知，本文提出的方法与前人的研究成果在模型思想与预测方法上有本质区别。经过仔细筛选和分析，文献[16]与[20]提出的预测方法与本文有一定的相似性，故从时间变量作用效果、路径可达概率量化有效性和预测准确性三个方面展开对比：

a)时间变量作用效果对比

对于 $PATH_3$ 中的子攻击 a8，攻击耗时约 110min，根据本文提出的方法计算出攻击意向为 0.16，所以攻击者放弃攻击节点从而路径 $PATH_3$ 不可达。而根据文献[20]的方法，攻击成本的值没有变化，不能体现出攻击耗时这一动态变量对于攻击可行性的影响。

文献[16]中使用时间增益补偿率量化时间的变化趋势，但是时间增益补偿率只用于攻击图优化，即用于定性分析节点是可达或者不可达。例如对于 $PATH_1$ 上的 a7 节点，在攻击耗时 40 分钟和攻击耗时 70 分钟两种情况下，根据文献[16]都可以得出攻击对应的子路径是可达的。但是对于可达的节点，文献[16]的方法不能体现攻击耗时的长短对于路径可达概率的影响程度的差异。

而根据本文提出的方法，可以计算出攻击耗时 40 分钟和耗时 70 分钟所对应的时间系数分别为 0.95 和 0.51，时间系数影响到攻击意愿取值，从而相应的路径可达概率也会存在差异。使用本文提出的引入了时间系数的攻击者意向量化方法，不仅可以定性地分析路径可达性，以达到消除冗余路径并优化攻击图的目的，也可以量化攻击耗时对路径可达概率的影响，使结果更加准确地反映出攻击耗时对于攻击行为的影响情况。

b)路径可达概率量化有效性对比

文献[20]提出的代价-收益模型与本文的攻击意向量化模型都用于评估子路径的攻击可行性。其中代价-收益模型中攻击代价的数据来源是 NVD 漏洞数据库，收益数据来源于资产价值，这些数据都是静态的，不能刻画出攻击场景随时间发生的动态变化对于路径可达性的影响。本文提出的方法对影响路径可行性的因素考虑更加全面，不仅包含了静态因素如漏洞本身的属性，资产价值等，也包含了攻击耗时和攻击者能力等动态因素。

此外，文献[20]在计算路径可达概率时，规定目标节点的可达概率等于所有直接和间接父节点的可达概率递归相乘，相当于将所有与目标节点相连的路径的可达性概率做了逻辑运算中的“与”运算。但这种方法适合于评估各节点的安全性，对于路径预测来说，概率累乘方法计算出的路径可达概率偏高，并且路径与路径之间可达性的差距更小，使得管理员判断出风险路径的难度增大。实际上攻击者一般只会选择一条路径攻击，而本文根据 IntenAbi-PathPre 算法对各路径的可达概率分别计算，通过横向比较路径上各节点的可达概率，从而得出攻击者最有可能攻击的路径，更加符合攻击行为的一般规律。

c)预测准确性对比

为了说明使用本文方法预测攻击路径的准确性，进行了多次实验，模拟攻击过程并采集相关数据，然后将得到的数据输入到预测模型当中。并与文献[20]和[16]的预测结果对比，实验结果如下：

表 7 路径预测性能对比

Tab. 7 Comparison of predicted performance

实验次数	文献[20]	文献[16]	本文
50	90.30%	92.50%	94.10%
100	92%	95.40%	97%
150	91.20%	93.80%	96.60%
200	94.40%	94.60%	95%
300	93.65%	95.25%	97.59%
500	95.50%	95.70%	98.40%

从表 7 可以看出，随着实验次数的增多，本文提出的预测方法准确率逐渐上升，并且相比于文献[20]和[16]仍有提升，这是因为本方法充分考虑到路径之间的差异性，将风险、攻击者能力、攻击耗时和攻击收益作为影响攻击意向进而影响攻击可行性的因素统筹考虑，并且根据攻击者能力调整漏洞可利用性分布，从而计算得出路径预测结果。通过这些改进，确保了预测方法的高效性。

4 结束语

在攻击手段越来越复杂多变的今天，如何有效预测攻击路径，精准识别攻击者的意图，从而为网络安全防护提供参考，是一个需要解决的问题。本文将实体网络的要素建模，使用攻击图描述攻击与资源之间的关系。根据攻击者的行为对攻击者能力进行区分并加以量化。提出攻击者意向的概念，并在对意向的量化中加入时间衰减因子，从攻击者主观意向的角度对路径可达性作出合理判断，实现了对攻击图的优化和对路径的预测，为网络管理员提供参考依据。

参考文献：

[1] 国家计算机网络应急技术处理协调中心. 2018 年我国互联网网络安全态势综述 [EB/OL]. (2019-04-17) http://www. cac. gov. cn/2019-04/17/c_1124379080. htm (National Internet Emergency Center.

Summary of Internet Security Situation in China in 2018 [EB/OL]. http://www. cac. gov. cn/2019-04/17/c_1124379080. htm)

[2] Radware. Global Application & Network Security report 2018-2019 [EB/OL]. (2019-04-03) https://www. radware. com/ert-report-2018

[3] Phillips C A, Swiler L P. A Graph-based System for Network-vulnerability Analysis [J]. Proceedings of the Workshop on New Security Paradigms, 1998: 71-79.

[4] Munoz-Gonzalez L, Sgandurra D, Barrere M, *et al.* Exact Inference Techniques for the Analysis of Bayesian Attack Graphs [J]. IEEE Transactions on Dependable and Secure Computing, 2017: 1-1.

[5] Shameli-Sendi A, Dagenais M, Wang L. Realtime Intrusion Risk Assessment Model based on Attack and Service Dependency Graphs [J]. Computer Communications, 2018 (116) , 253-272.

[6] 高岭，王帆，高妮，等. 基于改进蚁群算法的防护策略选择模型 [J]. 计算机工程与应用, 2019, 55 (07): 100-107. (Gao Ling, Wang Fan, Gao Ni, *et al.* Protection Strategy Selection Model Based on Improved Ant colony Algorithm [J]. Computer Engineering and Applications, 2019, 55 (07): 100-107.)

[7] 胡浩，叶润国，张红旗，等. 基于攻击预测的网络安全态势量化方法 [J]. 通信学报, 2017, 38 (10): 122-134. (Hu Hao, Ye Runguo, Zhang Hongqi, *et al.* Quantitative Method of Network Security Situation Based on Attack Prediction [J]. Journal of Communications, 2017, 38 (10): 122-134.)

[8] 叶子维，郭渊博，王宸东，等. 攻击图技术应用研究综述 [J]. 通信学报, 2017, 38 (11): 121-132. (Ye Ziwei, Guo Yuanbo, Wang Chendong, *et al.* Review of Attack Graph Technology [J]. Transactions of Beijing Institute of Technology, 2017, 38 (11): 121-132.)

[9] 秦虎，王建利，彭逍遥. 基于权限提升矩阵的攻击图生成方法 [J]. 北京理工大学学报, 2019, 39 (01): 101-105. (Qin Hu, Wang Jianli, Peng Xiaoyao, *et al.* Attack Graph Generation Method Based on Privilege Lifting Matrix [J]. Transactions of Beijing Institute of Technology, , 2019, 39 (01): 101-105.)

[10] Ghasemigol M, Ghaemi-Bafghi A, Takabi H. A Comprehensive Approach for Network Attack Forecasting [J]. Computers & Security, 2015, 58: 83-105.

[11] Bi K, Han D, Wang J. K maximum probability attack paths dynamic generation algorithm [J]. Computer Science and Information Systems, 2016, 13 (2): 677-689.

[12] 高妮，高岭，贺毅岳，等. 基于贝叶斯攻击图的动态安全风险评估模型 [J]. 四川大学学报（工程科学版）, 2016, 48 (01): 111-118. (Gao Ni, Gao Ling, He Yiyue, *et al.* Dynamic Security Risk Assessment Model Based on Bayesian Attack Graph [J]. Journal of Sichuan University (Engineering Science Edition) , 2016, 48 (01): 111-118.)

[13] 胡浩，刘玉岭，张红旗，等. 基于吸收 Markov 链的网络入侵路径预测方法 [J]. 计算机研究与发展, 2018, 55 (04): 831-845. (Hu Hao, Liu Yuling, Zhang Hongqi, *et al.* Network Intrusion Path Prediction Method Based on Absorbing Markov Chain [J]. Journal of Computer Research and Development, 2018, 55 (04): 831-845.)

[14] Dewri R, Ray I, Poolsappasit N, *et al.* Optimal security hardening on attack tree models of networks: a cost-benefit analysis [J]. International Journal of Information Security, 2012, 11 (3): 167-188.

[15] Dai F, Hu Y, Zheng K, *et al.* Exploring risk flow attack graph for security risk assessment [J]. Iet Information Security, 2015, 9 (6): 344-353.

[16] 王辉，王银城，鹿士凯. 基于时间增益补偿率的攻击路径优化算法 [J]. 计算机工程, 2018, 44 (08): 184-191+198. (Wang Hui, Wang Yincheng, Lu Shikai. Attack Path Optimization Algorithm Based on Time Gain Compensation rate [J] , Computer Engineering, 2018, 44 (08): 184-191+198.)

[17] HOMER J, ZHANG S, OU X, *et al.* Aggregating vulnerability metrics in enterprise networks using attack graphs [J]. Journal of Computer Security, 2013, 21 (4): 561-597.

[18] 王硕，汤光明，寇广，等. 基于因果知识网络的攻击路径预测方法 [J]. 通信学报, 2016, 37 (10): 188-198. (Wang Shuo, Tang Guangming, Kou Guang, *et al.* Attack Path Prediction Method Based on Causal Knowledge Network [J]. Journal of Communications, 2016, 37 (10): 188-198.)

[19] Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system [J]. IEEE Security & Privacy Magazine, 2006, 4 (6): 85 – 89.

[20] 高妮，高岭，贺毅岳，王帆. 基于贝叶斯攻击图的最优安全防护策略选择模型 [J]. 计算机工程与应用, 2016, 52 (11): 125-130. (Gao Ni, Gao Ling, He Yiyue, *et al.* The Model of Selecting The Best Security Policy Based on Bayesian Attack Graph [J]. Computer Engineering and Applications, 2016, 52 (11): 125-130.)